House Bill 276

By: Representatives Setzler of the 35th, Hill of the 21st, Brooks of the 63rd, and Loudermilk of the 14th

A BILL TO BE ENTITLED

AN ACT

To amend Title 10 of the Official Code of Georgia Annotated, relating to commerce and trade, so as to provide a short title; to provide for definitions; to set forth the purposes of the Biometric Information Protection Act; to provide for civil and criminal penalties; to provide for venue; to prohibit the use of genetic information for the issuance of life insurance; to prohibit the use of genetic information in employment decisions; to prohibit the use of biometric information in enrollment decisions in educational institutions; to provide for information on public and private identification and access cards; to define certain unfair business practices for preferential treatment of customers that reveal biometric information; to prohibit the implanting of biometric sensors or personal location tracking devices; to provide for the release of biometric or genetic information to legal authorities; to provide for related matters; to provide for an effective date; to repeal conflicting laws; and for other purposes.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF GEORGIA:

SECTION 1.

Title 10 of the Official Code of Georgia Annotated, relating to commerce and trade, is amended by adding a new chapter to read as follows:

"CHAPTER 12A

10-12A-1.

This chapter shall be known and may be cited as the 'Biometric Information Protection Act.'

10-12A-2.

As used in this chapter, the term:

(1) 'Administrator' means the administrator of the 'Fair Business Practices Act of 1975' appointed pursuant to subsection (a) of Code Section 10-1-395, or the administrator´s designee.

(2) 'Biometric information' means any indelible personal physical characteristic which can be used to uniquely identify an individual or pinpoint an individual at a particular place at a particular time. Examples of biometric information shall include, but not be limited to, fingerprints, information from biometric sensors, deoxyribonucleic acid (DNA) samples, retinal scans, palm or hand prints, and X-rays or similar indelible physical images or representations. For purposes of this Code section, written signatures and photographs shall not be considered biometric information.

(3) 'Biometric sensor' means an implanted device or sensor that tracks or monitors an individual´s vital signs or personal physical information including, but not limited to, heart rate, blood pressure, or blood alcohol content.

(4) 'Collector of biometric information' means any group, association, corporation, governmental or private entity or agency, individual, or person that collects, stores, maintains, or transmits biometric information.

(5) 'Genetic testing' means laboratory tests of human DNA or chromosomes for the purpose of identifying the presence or absence of inherited alterations in genetic material or genes which are associated with a disease or illness that is asymptomatic at the time of testing and that arises solely as a result of such abnormality in genes or genetic material. For purposes of this chapter, genetic testing shall not include routine physical measurements; chemical, blood, and urine analysis; tests for abuse of drugs; and tests for the presence of the human immunodeficiency virus.

(6) 'Individual' means any natural person who is the subject of the collection of biometric information.

(7) 'Insurer' means an insurer, a fraternal benefit society, a nonprofit medical service corporation, a health care corporation, a health maintenance corporation, or a self-insured health plan not subject to the exclusive jurisdiction of the Employee Retirement Income Security Act of 1974, 29 U.S.C. Section 1001, et seq.

(8) 'Personal location tracking technologies' means any device which allows access to information pinpointing an individual at a particular location at a specific point in time. This includes, but is not limited to, global positioning systems (GPS) tracking chips or radio frequency identification (RFID) devices.

(9) 'Personal or unique identification information' means information such as an individual´s name, address, telephone number, driver´s license number, and social security number.

(10) 'Record' means any material on which written, drawn, printed, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.

10-12A-3.

(a) Any group, association, corporation, entity, individual, or person shall follow these guidelines when collecting and storing biometric information:

(1) The fact that the biometric information is being collected or stored must be revealed to the individual and the individual must sign a written consent allowing the collection or storage of his or her personal biometric information;

(2) The specific purpose for which the biometric information is being collected or stored must be revealed to the individual and the individual must sign a written consent allowing the use of his or her biometric information for such purpose;

(3) Prior to sharing any biometric information with any third party by a collector of biometric information, the third party must reveal the specific purpose for which the biometric information is to be used and the third party must obtain the written consent of the individual allowing such use of his or her biometric information;

(4) The collector of the biometric information shall have the duty to protect the information from unauthorized access and must develop a written policy, which is made available to the individual, establishing guidelines for destroying the biometric information when its initial specific purpose has been satisfied or within three years of the individual´s last transaction with the collector; and

(5) The collector of the biometric information may share such information only with a government entity or agent upon the government entity or agent presenting a valid search warrant, based upon probable cause and issued by a court of competent jurisdiction.

(b) The provisions of this Code section shall not apply to collection of biometric information by a law enforcement officer or agency pursuant to a warrant issued by a court of competent jurisdiction.

10-12A-4.

(a) An individual whose biometric information is negligently, recklessly, or intentionally compromised and subsequently used in an unauthorized fashion and who suffers harm as a result of the unauthorized use of such information may recover or obtain any or all of the following against the person who allowed the compromise of the biometric information:

(1) Actual damages;

(2) Equitable relief, including, but not limited to, an injunction or restitution of money or property;

(3) Punitive damages under the circumstances set forth in Code Section 51-12-5.1;

(4) Reasonable attorneys´ fees and expenses; and

(5) Any other relief which the court deems proper, including an order to correct a public or private record that contains biometric information obtained through any violation of this chapter.

(b) Any attempt to violate this chapter, or any violation of this chapter, that causes damages of less than $500.00 shall be a misdemeanor. Any attempt to violate this chapter, or any violation of this chapter, that causes damages of $500.00 or more shall be a felony, punishable by a fine of up to $5,000.00 and imprisonment of up to three years, or both. The court shall use its discretion and base the sentence and fine on the severity of the offense and the amount of damage caused thereby.

(c) Victims of violations of this chapter may bring a class action, if otherwise proper under Code Section 9-11-23, to enforce the provisions of this chapter.

(d) Each violation of this chapter shall constitute a separate offense.

(e) The Attorney General and prosecuting attorneys shall have the authority to conduct the prosecution for a violation of this chapter.

(f) The administrator shall have the authority to investigate alleged violations of this chapter, including all investigative powers available under the 'Fair Business Practices Act of 1975,' Code Section 10-1-390, et seq., including, but not limited to, the power to issue investigative demands and subpoenas as provided in Code Sections 10-1-403 and 10-1-404.

(g) Nothing contained in this Code section precludes law enforcement agencies from investigating violations of this chapter.

(h) The rights and remedies contained in this Code section shall not be subject to waiver.

10-12A-5.

Any insurer doing business in the State of Georgia is prohibited from requiring any information derived from genetic testing to determine an applicant´s eligibility for life insurance or to determine the rates to be charged for the life insurance. However, any preexisting information derived from genetic testing must be supplied to the insurance company when applying for a life insurance policy.

10-12A-6.

No employer or employment agency, public or private, operating in the State of Georgia shall use for identification purposes or require as a condition of employment:

(1) Information derived from genetic testing;

(2) Biometric information other than genetic testing; provided, however, that this condition may be waived when necessary for employment in positions that involve unaccompanied access to high security areas, intelligence information, or children;

(3) Any information derived from biometric sensors; or

(4) Any information derived from personal location tracking technologies.

10-12A-7.

No educational institution, public or private, operating in the State of Georgia shall require any of the following as a condition of enrollment:

(1) Information derived from genetic testing;

(2) Biometric information other than genetic testing;

(3) Any information obtained from biometric sensors; or

(4) Any information derived from personal location tracking technologies.

10-12A-8.

(a) Government issued identification or access cards or devices shall not contain:

(1) Biometric information;

(2) Personal or unique identification information, biometric information, or medical information that is remotely readable without the card or device holders´ knowledge or consent; or

(3) Technologies that allow the card or device to be physically tracked.

(b) Privately issued identification or access cards or devices shall not contain:

(1) Personal or unique identification information, biometric information, or medical information that is remotely readable without the card or device holders´ knowledge or consent; or

(2) Technologies that allow the card or device to be tracked off the physical premises of the private organization´s primary place of business.

(c) The provisions of this Code section shall not apply to devices that are not implanted and are being used pursuant to a judicial order, as a condition of probation or parole, or to monitor a sex offender.

10-12A-9.

(a) It is an unfair business practice in the State of Georgia to require or offer preferential treatment, access, or pricing for individuals that consent to the collection of biometric information in order to:

(1) Make a sales transaction;

(2) Make a financial transaction, other than allowing a bank to require a fingerprint or hand print before issuing cash to a nonaccount holder or allowing unsupervised access to a secure controlled area, such as an area containing safe-deposit boxes; or

(3) Gain access to public or private property that is generally accessible to the public with or without an admission charge.

(b) It is an unfair business practice in the State of Georgia to give or offer preferential treatment of any kind to individuals who allow personal biometric information to be collected as opposed to individuals who refuse to allow the collection of personal biometric information.

10-12A-10.

(a) Implanted personal biometric sensors, personal location tracking technologies, or any similar devices shall not be required to be implanted in any individual without the individual´s consent.

(b) The voluntary implantation of any microchip or similar device shall be regulated under the authority of the Composite Board of State Medical Examiners.

10-12A-11.

(a) Notwithstanding the provisions of Code Section 33-54-5, biometric information or information derived from genetic testing shall not be disclosed to legal authorities conducting an investigation or prosecution without an appropriate warrant showing probable cause issued by a court of competent jurisdiction.

(b) The State of Georgia or any of its political subdivisions, agencies, or agents is allowed to collect appropriate samples and analyze information derived from genetic testing from convicted felons only, unless they obtain the consent of the individual, collect it as abandoned evidence, or obtain an appropriate warrant showing probable cause issued by a court of competent jurisdiction. A sample from a convicted felon may be collected upon the conviction becoming final and may be compared against an unsolved crimes data base.

(c) The State of Georgia or any of its political subdivisions, agencies, or agents shall not enter genetic information into a data base or deliver genetic information to other governmental entities until the subject individual has been convicted of a felony and exhausted all rights of appeal.″

SECTION 2.

This Act shall become effective on July 1, 2007.

SECTION 3.

All laws and parts of laws in conflict with this Act are repealed.